STOP, You're on Camera

Al-Sharieh, Saleh; Mifsud Bonnici, Jeanne

Published in:
Synergy of Community Policing and Technology

DOI:
10.1007/978-3-030-00299-2_4

Publication date:
2019

STOP, You're on Camera: The Evidentiary Admissibility and Probative Value of Digital Records in Europe

Saleh Al-Sharieh and Jeanne Mifsud Bonnici

Introduction

Law is the tool defining the content of rights and obligations especially in democratic societies (Clark 1942). As part of this role, the branch of criminal law specifies the actions and omissions that constitute crimes, along with their respective punishment, and describes the procedures that the State must follow in the investigation and prosecution of persons accused of criminal offences, who are presumed innocent until proven guilty (Universal Declaration of Human Rights 1948, art.11). Proving an accused's guilt is generally the task of the State and occurs by furnishing "evidence", which is "pertinent information sufficient to persuade the trier of fact to form a belief that the accused is guilty to some specified standard of certainty, traditionally expressed in criminal proceedings as 'proof beyond reasonable doubt'" (Roberts and Zuckerman 2010, p. 96).

The revolution in computing and telecommunication technologies has impacted criminal law. Computers and networks have become a target to criminals and one of the tools they use to commit or facilitate their crimes (McQuade 2006). These developments have created challenges to the law of evidence, which has relied upon the

This chapter is based on the research done for the Citizen Interaction Technologies Yield Community Policing (CITYCoP) project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653811.

S. Al-Sharieh (✉)
Department of Private Law, College of Law, United Arab Emirates University (UAEU), Al Ain, Abu Dhabi, UAE
e-mail: saleh.al-sharieh@uaeu.ac.ae

J. M. Bonnici
Department of Transboundary Legal Studies, Faculty of Law, University of Groningen, Groningen, The Netherlands

G. Leventakis, M. R. Haberfeld (eds.), *Synergy of Community Policing and Technology*, SpringerBriefs in Criminology, https://doi.org/10.1007/978-3-030-00299-2_4

technological neutrality of its doctrines to cope (Law Reform Commission 2009). Nevertheless, today's advancement and widespread of mobile computing and wireless networks have created opportunities for evidence law (Byrne and Marx 2011). Sometimes, an individual captures a picture or video that proves useful in detecting a crime offender and/or proving her/his guilt (Rentschler 2016). This video or picture is digital evidence: "information and data of value to an investigation that is stored on, received, or transmitted by an electronic device" (National Institute of Justice 2008, p. ix). Evidence has increasingly become digital in nature and law enforcement agencies (LEAs), lawyers, and courts have increasingly encountered digital evidence issues in the course of their duties (Casey 2011). Yet, legal systems still apply the rules of traditional evidence to the issues raised by digital records (Insa 2007). This is problematic given the difficulty associated with proving the authenticity and reliability of digital records. Evidence is the cornerstone of any trial (Leroux 2004). It is therefore important to ensure that a reasonable level of certainty exists with regard to its admissibility and probative value when it is digital. Also, it is important to equip digital community policing systems with the technical and institutional safeguards necessary to meet the requirements of the law of evidence.

Applying a legal doctrinal method, this chapter unfolds the legal rules of evidence that should inform the design of technology-enabled community policing systems to embody safeguards to protect the admissibility and probative value of the records that they collect, transmit and store. Following this introduction, the Chapter discusses the main approaches to the regulation of evidence in Europe and highlights the specific admissibility and probative value challenges facing records collected, transmitted or stored by digital community policing systems.

The Rules of Criminal Evidence: The Three Approaches in Europe

There are three approaches to the rules of criminal evidence in Europe: (1) The freedom of evidence principle; (2) the freedom of evidence principle along with rules limiting the discretion of the court; and (3) detailed rules of evidence (Williams 1998).

Freedom of Evidence

As a general rule, judges can form their inner conviction about the guilt or innocence of the accused by relying on any piece of evidence presented and discussed before them. There are no specific rules regarding the sources, types, admissibility or weight of evidence that the judges must use to reach a verdict of innocence or

guilt. France is an example of the jurisdictions following this approach. According to article 427 of the French Code of Penal Procedure (CPP), "[e]xcept where the law otherwise provides, offences may be proved by any mode of evidence and the judge decides according to his innermost conviction". This practically means that judges can admit digital evidence as well as evidence such as hearsay testimony—"[w]ritten or oral statements or communicative conduct made by persons otherwise than in testimony at the proceedings in which it is offered" (Sopinka 1999, p. 173)—that is usually excluded by the rules of evidence in jurisdictions such as the United States (Frase 1990). Under the freedom of evidence principle, all evidence including confession is subject to the evaluation of the judge.

The freedom of evidence principle also applies in trials before the Assize Court (cour d'assises), which is the main criminal court in France and the only one that operates with a jury (Woods 1931). Article 353 of the French CPP liberates the judges of the court from following specific rules regarding the fullness or adequacy of evidence but requires them "to seek in the sincerity of their conscience what impression has been made on their reason by the evidence brought against the accused and the arguments of his defence" and to answer the following question: "are you inwardly convinced?"

The principle of freedom of evidence gives judges enough flexibility to consider whatever available information might be useful to reach a verdict about the guilt or innocence of the accused without being overburdened by written rules (Williams 1998). This ensures that criminals will not escape a verdict of guilt by virtue of a loophole in the procedural rules of evidence (Stannard 2015). It in addition helps expedite trial time by limiting the opportunities in which lawyers can attempt to invoke rules on evidence exclusion (Williams 1998). On the other hand, the principle of freedom of evidence may create uncertainty in criminal proceedings and may encourage the filling of cases even in the absence of material evidence (Wigmore 1942; Williams 1998).

It is logical for the French criminal justice system to adopt the principle of freedom of evidence, because it assigns fact-finding to professional judges, who have legal education and training, rather than to jurors, except in the Assize Court (Williams 1998). France adopts the inquisitorial legal system in which judges play an active role in investigating the facts of the case to develop a personal opinion about truth (Pugh 1962).

The principle of freedom of evidence is not without limitations. For instance, article 432 of the French CPP explicitly prohibits deriving written evidence from the correspondence exchanged between the accused and his/her lawyer. Similarly important, courts can exclude evidence whose collection does not conform to prescribed procedures when the law prescribes the penalty of nullity as a remedy of such violation and when the violation damages the interests of the accused. For instance, according to article 179 of the French CPP, "[t]here is a nullity when the breach of an essential formality provided for by a provision of the present Code or by any other rule of criminal procedure has harmed the interests of the party it concerns". This form of exclusion, referred to as substantial nullity (nullités substantielle), is difficult to categorize and is decided by courts on a case-by-case basis

(Hodgson 2005). In contrast, in a number of provisions, the French CPP provides that the violation of a given procedure, such as the ones designed to protect the rights of individuals during domicile search, will result in nullity. For example, article 59 provides "[t]he formalities mentioned under articles 56, 56-1, 57 and the present article are prescribed under penalty of nullity". This form of nullity is referred to as textual nullity (nullité textuelle) (Rengel 2013). There have been many occasions when the court of Cassation excluded evidence not obtained in conformity with the procedures prescribed in the French CCP (Buisman et al. 2010). Further, courts would exclude confessions extracted by the police through subjecting the accused to physical abuse (Ma 1999). As a result, legality is explicitly an element of evidence admissibility in specific circumstances and in general an element that judges will unlikely overlook when formulating their "innermost conviction" about the innocence or guilt of the accused (Leroux 2004).

Besides the requirement of legality, there are other requirements that impact the admissibility or weight of a given record as evidence under the French CPP: namely the relevance requirement as well as the authenticity and reliability requirement.

A relevant fact is that "either taken by itself or in connection with other facts proves or renders probable the past, present, or future existence or non-existence of [another fact]" (Stephen 1886, p. 2). While the French CPP does not explicitly require the evidence to be relevant in order to be admissible, several provisions in it impliedly refer to this requirement. For example, the President of the Assize Court has the power to exclude irrelevant records by virtue of article 309. Similarly important, the requirement of relevance stems from logic (Thayer 1898; Nzjboer 2000). It is a necessary requirement for the right answer to the inquiry (Tillers and Schum 1991). Judges have a wide power of discretion to evaluate the relevance of the record by virtue of article 427 of the French CPP (Pradel 2000; Leroux 2004).

As to the authenticity and reliability requirement, generally a record is authentic if it is the record that it purports to be and is reliable if it is trustworthy: "it can be treated as a fact in itself" (Duranti 1995, p. 6–7). To be authentic, the record must remain unchanged; it must originate from its claimed source; and its extraneous information, such as its date, must be accurate (Reed 1990). The record receives its reliability from the form and procedures of its creation (Duranti 1995). The date and signature are traditionally the required elements in the form (Ibid). They link the record, specifically the information or acts contained therein, to its maker and make him/her responsible for its content (Ibid). Meanwhile, the procedures of creation refer to the different rules regulating how the information or acts are recorded, such as the rules assigning the competence to make the record or specifying how it is handled (Ibid).

Several provisions in the French CPP refer to the authenticity and integrity requirement of evidence, including digital evidence. For instance, article 537 considers official records and reports produced by, inter alia, judicial police officers "prima facie *authentic* evidence" [emphasis added]. Further, articles 56 and 97 prescribe specific measures to be followed in the process of collecting documents or electronic data during an authorized seizure: For instance, (1) only specifically authorized persons are allowed to examine the documents or electronic data before

seizing them; (2) documents and items seized must be promptly entered on an inventory and kept in a judicial safekeeping under official seals; (3) when the seizure involves electronic data, the seizure occurs by seizing the physical medium containing the data or by making a copy of the data in the presence of the person(s) carrying out the seizure.

The issue of the authenticity and reliability of a record is inherently connected to the inner conviction of the reasonable judge who, in light of the freedom of evidence principle, will have the full discretion in its determination.

Rules of Evidence

The principle of freedom of evidence is familiar to other jurisdictions in continental Europe, such as Germany. Section 244(2) of the German Code of Criminal Procedure (StPO) provides that "[i]n order to establish the truth, the court shall, *proprio motu*, extend the taking of evidence to all facts and means of proof relevant to the decision". Yet, the StPO subjects the principle to greater limitations than those existing under the French law by providing rules directing judges with regard to evaluating the evidentiary admissibility and probative value of a record. The evidence rules are designed to address common evidence law problems that judges encounter in criminal cases and that would otherwise require extra efforts to address (Williams 1998). In addition, this approach keeps to judges enough flexibility to tailor the use of the evidence in a way responsive to the specific facts of the case (Ibid). The rules on witness evidence in sections 48-71 of the StPO are a good illustration of the extent to which it details the rules on the admission and administration of a type of evidence. For example, section 68a of the StPO directs the court with regard to the questions that are to be and not to be asked.

Under the StPO, relevance is a requirement for the evidence admissibility. Section 244(3) requires the judge to refuse the application to take evidence when "the taking of such evidence is superfluous because the matter is common knowledge, the fact to be proved is irrelevant to the decision or has already been proved, the evidence is wholly inappropriate or unobtainable, the application is made to protract the proceedings, or an important allegation which is intended to offer proof in exoneration of the defendant may be treated as if the alleged fact were true".

Arguably other provisions in the StPO include a legality requirement although the StPO does not have a general exclusionary rule regarding illegally gathered evidence (Gless 2010). For instance, section 136a provides that "[t]he accused's freedom to make up his mind and to manifest his will shall not be impaired by ill-treatment, induced fatigue, physical interference, administration of drugs, torment, deception or hypnosis" and that "[m]easures which impair the accused's memory or his ability to understand shall not be permitted". Accordingly, courts will exclude confessions obtained by means of the violations described in the section (Gless 2010). Overall, the StPO evidence rules must be read along with the rules protecting

individuals' rights and freedoms in the Basic Law of Germany, such as the right to privacy in article 10.

The StPO does not explicitly address the authenticity and reliability of evidence requirements. However, section 93 describes the measures to be followed in order to verify the authenticity and reliability of a document, specifically by requiring a handwriting comparison to be conducted by experts. As to electronic records, section 41a(1) of the StPO allows for the admission of electronic documents as equivalent to documents if they carry an electronic signature, following the requirements of the Digital Signatures Act, and are suitable for processing by the court. Moreover, besides electronic signatures, the section speaks about the possibility of another statute providing for "the admissibility of a further secure procedure which guarantees the authenticity and the integrity of the electronic document transmitted". In Germany, by virtue of section 244(2) of the StPO, courts will "extend the taking of evidence to all facts and means of proof relevant to the decision". Hence, they will not automatically exclude evidence whose authenticity and reliability is questionable (The Law Commission 1995). Authenticity and reliability will impact the probative value of the evidence rather than its admissibility (Ibid).

Detailed Rules of Evidence

In several European countries, such as England and Romania, evidence law includes very detailed rules regarding the admissibility and probative value of evidence. In principle, the English law of evidence admits all evidence as long as it is relevant and not excluded from admissibility by a statutory or common law exclusionary rule or by the discretion of the judge (Keane and McKeown 2016; Leroux 2004). Accordingly, evaluating the evidentiary admissibility of a record involves three inquiries: whether the record is relevant or not; whether it is excluded by an applicable exclusionary rule; and whether there is any inclusionary exception on the exclusionary rule (Roberts and Zuckerman 2010). The English law of evidence has several exclusionary rules. For instance, according to section 76 of the Police and Criminal Evidence Act 1984 (PACE), the court must exclude a confession, even if it is true, when it appears to the court that it was obtained by oppression or was a result of "anything said or done" which was likely to make it unreliable, unless the prosecutor relying on the confession proves to the court beyond reasonable doubts that it was not obtained through those means. Furthermore, section 78 of PACE authorizes the court to exclude unfair evidence.

This is not to say that the English law of evidence has a general legality requirement. Case law has often held that relevance is the only requirement of admissibility while legality is not. In *Kuruma v The Queen* (1955, A.C. 197, p. 203) the House of Lords held that "the test to be applied in considering whether evidence is admissible is whether it is relevant to the matters in issue. If it is, it is admissible and the court is not concerned with how the evidence was obtained". In fact, according to section s.76(4) of PACE, even when the court excludes a confession, this will not impact the

admissibility of any evidence relating to a fact discovered because of the confession.

When a rule of evidence excludes a specific type of evidence, courts will accept it if it is subject to an exception to the exclusionary rule. For instance, section 114 of the Criminal Justice Act 1988 (CJA) provides that hearsay evidence is admissible only when it falls under one of the four exceptions provided in the section, such as when all the parties of the proceedings accept its admissibility or when the court is convinced that its admission is "in the interests of justice".

As to the authenticity and reliability of evidence, the English law does not statutorily address the issue and courts have usually referred to it briefly (Pattenden 2009). Nonetheless, it is arguable that courts will not admit evidence whose authenticity and reliability are questionable unless there is a legal presumption of authenticity or an agreement to this effect, especially given the strong link between relevance and authenticity (Ibid).

In Romania, the Criminal Procedure Code (CPC) includes very detailed rules on the types of evidence accepted in criminal proceedings, the conditions for its admission, and the remedy available to the parties of the proceedings when the collection of the evidence does not conform to the conditions prescribed in the law. More specifically, the CPC places the judicial bodies under an obligation to find the truth about the facts of a case or about the suspect by relying on evidence (Romanian CPC, art.5). It allows any means not prohibited by law to be used for collecting evidence including statements made by suspects or defendants; statements made by victims; statements made by witnesses; and documents, expert reports, pictures, and physical evidence (Romanian CPC, art. 97(2)). The CPC requires the evidence to be both relevant and obtained by legal means to be admissible: a judicial body may exclude evidence when it is irrelevant, unnecessary, impossible to obtain or contrary to the law (Romanian CPC, art.100). In the same vein, the CPC prohibits the use of violence or any coercion in obtaining evidence (Romanian CPC, art. 101). This prohibition extends to cover the use of entrapment for the purpose of collecting evidence and the use of any means that may affect the person's capacity to remember or tell conscientiously and voluntarily facts that can be object of evidence (Romanian CPC, art. 101). By virtue of article 102, courts will exclude evidence unlawfully obtained.

The CPC does not include a general rule regarding the authenticity and reliability of evidence. Hence, courts will have the discretion to determine the admissibility or value of the record whose authenticity or reliability is uncertain (Romanian CPC, art. 103). However, the CPC refers to the process to be followed in order to ensure the authenticity and reliability of records of electronic surveillance activities (Romanian CPC, art. 143). Article 138(b) of the CPC treats video, audio or photo surveillance as a special method of investigation, and LEAs will have to obtain a court order to authorize it after the statutory conditions for granting this order have been fulfilled.

Digital Evidence Challenges

Users of digital community policing systems can transmit digital records, such as videos and pictures, through their mobile devices in the processes of reporting a danger or offence. These records can be useful tips that lead LEAs to conduct investigations and possibly collect other relevant records to the investigations (Burns and Conte 2014; Shifrin 1991). Later, prosecutors may rely on such records to establish the guilt of an accused before a court. At this stage, the question of the admissibility and probative value of those records arises. As the discussion in the previous section shows, relevance of the records to the proceedings is key for their admissibility. Legality of the records is a requirement for their admissibility in some jurisdictions and authenticity and reliability will impact their probative value although statutes do not instruct courts to exclude evidence whose authenticity and reliability are not established (Allegrezza 2010). Generally, European jurisdictions do not subject digital evidence to different rules (Insa 2007). Therefore, it has to meet the requirements of the admissibility of traditional evidence and is subject to the same factors impacting the probative value of the latter (Leroux 2004).

Establishing the authenticity and reliability of digital evidence is challenging:

> [T]he easiness of electronic records creation and the level of autonomy that it has provided to records creators, coupled with an exhilarating sense of freedom from the chains of bureaucratic structures, procedures, and forms, have produced the sloppiest records creation ever in the history of record making. Too many persons and too many records forms generated in too many different contexts participate in the same transaction; too much information is recorded; too many duplicates are preserved; and too many different technologies are used. In other words; electronic records, as presently generated, might be authentic, but they are certainly not reliable (Duranti 1995, p. 9).

The uncertainty regarding the identity of the author of the digital record sheds doubts on its authenticity (Chaski 2005; Thomson 2013; Brown 2015). Furthermore, given the fragility of the digital record and its vulnerability to alteration, it is difficult to ensure that it has not been manipulated or altered after its creation (Kerr 2001; Brown 2015; Solon and Harper 2004). Theoretically, prosecutors may overcome this challenge by proving the chain of custody of the record (Dubord 2008; Brown 2015), which is "a process used to maintain and document the chronological history of the evidence;" (Brenner 2004, p.54). It documents the details of every instance of interaction with the record: when, where, why and how the record is accessed or used and by whom (Giova 2011). Practically, however, proving a chain of custody of a digital record that has not been violated from the moment of the creation of the record to the moment of its presentation in the court is difficult (Brown 2015; Insa 2007).

Moreover, establishing the reliability of the digital device that has produced the digital record is another challenge facing the authenticity and reliability of digital evidence. It is important to ensure that the electronic device or any of the programs responsible for producing, transmitting or preserving the digital record has been free from any defects or intrusions that could have compromised its integrity

(Thomson 2013). Finally, ensuring the completeness of the digital record is problematic because there is a risk that it does not include all the actions or events it purports to capture (Ibid).

The difficulty associated with proving the authenticity and reliability of digital records does not mean courts will exclude them at the outset. In England, for instance, digital records have been admitted "as evidence that speaks for itself" (Pattenden 2009). Equally important, securing the authenticity and reliability of digital records is technologically feasible as the research in this field illustrates (Kuntze et al. 2012).

Conclusion

Under the rule of law, the punishment of offenders is possible only when their guilt is proven before the judiciary in accordance with specific legal safeguards including the rules of evidence law, which are a set of legal and logical rules designed to ensure that no one is punished for a crime he/she did not commit. Digital community policing systems can help achieve the objective of this law. Users of these systems can collect, transmit and store digital records relevant to violations of law. LEAs can use these digital records as tips to collect further evidence and prosecutors can use them later to prove the guilt of an accused before courts. In the latter situation, it is necessary that the digital records meet the law requirements regarding the admissibility and probative value of evidence.

In Europe, different jurisdictions follow different approaches towards the regulation of the admissibility and evaluation of the probative value of evidence. For instance, France adopts the freedom of evidence principle by which a judge will reach a verdict of guilt or innocence of the accused by relying on any evidence presented and discussed in the trial. In a like manner, the law of evidence in Germany adopts the freedom of evidence principle but the StPO subjects the principle to more limitations than those existing under the French law. On the other hand, countries like Romania have very detailed rules on the types of evidence accepted in criminal proceedings, the conditions for its admission, and the remedy available to the parties of the proceedings when the collection of the evidence does not conform to the conditions prescribed in the law.

In Europe, jurisdictions do not subject digital evidence to different rules than those applicable to traditional evidence, such as written documents. Therefore, records collected, transmitted or stored by digital community policing systems will have to satisfy the requirements of relevance, legality, authenticity and reliability to be admissible and/or to have considerable probative value. In this regard, the authenticity and reliability requirement is the main challenge that the records will have to overcome. It is true that, as a general rule, jurisdictions do not statutorily exclude the admissibility of evidence when its authenticity and reliability are not established. Nevertheless, especially in the jurisdictions applying the freedom of evidence principle, the authenticity and reliability of evidence will have a great

influence on the courts' determination of the value of the evidence, given the connection between the authenticity and reliability of the evidence and other requirements of admissibility such as relevance. Therefore, to preserve the probative value of the digital records collected, transmitted or stored by digital community policing systems, the designers of these systems should consider overcoming the following challenges during the design and implementation:

- The challenge of authorship: The systems should incorporate a trait or mechanism that enables the identification of the source, the author or creator, of the records as well as the time, date and location of their creation.
- The challenge of alteration and manipulation: The systems should incorporate measures that protect the digital records from alteration, manipulation or damage during their collection, transmission or storage.
- The challenge of the reliability of the software and device involved in the creation, transmission or storage of the digital records: The systems should incorporate measures to ensure that the records created, transmitted or stored are what they purport to be.
- The challenge of completeness: The systems should incorporate measures that verify whether the digital records have suffered any omissions or they fully capture the actions or events they purport to capture.

References

Allegrezza, S. (2010). Critical remarks on the green paper on obtaining evidence in criminal matters from one member state to another and securing its admissibility. *Zeitschrift für Internationale Strafrechtsdogmatik, 9*, 569–579.

Brenner, J. C. (2004). *Forensic science: An illustrated dictionary*. London: CRC Press.

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*, 55–119.

Buisman, C., Bouazdi, M., & Costi, M. (2010). Principles of civil law. In K. A. A. Khan, C. Buisman, & C. Gosnell (Eds.), *Principles of evidence in international criminal justice* (pp. 7–95). Oxford: Oxford University Press.

Burns, T. H. C., & Conte, M. (2014). Terry stops, anonymous tips, and driving under the influence: A study of Illinois law. *Loyola University Chicago Law Journal, 45*, 1143–1193.

Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing. A review of the research on implementation and impact. *Cahiers Politiestudies Jaargang, 20*, 17–40.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet*. Waltham, MA: Academic Press.

Chaski, C. E. (2005). Who's at the keyboard? Authorship attribution in digital evidence investigations. *International Journal of Digital Evidence, 4*, 1–14.

Clark, C. E. (1942). The function of law in a democratic society. *University of Chicago Law Review, 9*, 393–405.

Dubord, P. (2008). Investigating cybercrime. In J. J. Barbara (Ed.), *Handbook of digital and multimedia forensic evidence* (pp. 77–89). Totowa, NJ: Humana Press.

Duranti, L. (1995). Reliability and authenticity: The concepts and their implications. *Archiv, 39*, 5–10.

Frase, R. S. (1990). Comparative criminal justice as a guide to American law reform: How do the French do it, how can we find out and why should we care? *California Law Review, 78*, 539–683.

Giova, G. (2011). Improving chain of custody in forensic investigation of electronic digital systems. *International Journal of Computer Science and Network Security, 11*, 1–9.

Gless, S. (2010). Truth or due process? The use of illegally gathered evidence in the criminal trial. In J. Basedow, U. Kischel, & U. Sieber (Eds.), *German National Reports to the 18th International Congress of Comparative Law* (pp. 675–709). Tübingen: Mohr Siebeck.

Hodgson, J. (2005). *French criminal justice: A comparative account of the investigation and prosecution of crime in France*. Oxford: Hart Publishing.

Insa, F. (2007). The admissibility of electronic evidence in court: Fighting against high-tech crime. *Journal of Digital Forensic Practice, 1*, 285–289.

Keane, A., & McKeown, P. (2016). *The modern law of evidence*. Oxford: Oxford University Press.

Kerr, O. S. (2001). Computer records and the Federal Rules of evidence. *United States Attorneys' USA Bulletin, 49*, 1–9.

Kuntze, N., et al. (2012). On the creation of reliable digital evidence. In G. Peterson & S. Shenoi (Eds.), *Advances in digital forensics* (pp. 3–17). London: Springer.

Law Reform Commission. (2009). *Documentary and electronic evidence*. Retrieved August 15, 2017, from http://www.lawreform.ie/_fileupload/consultation%20papers/cpdocumentaryandelectronicevidence.pdf

Leroux, O. (2004). Legal admissibility of electronic evidence. *International Review of Law Computers & Technology, 18*, 193–220.

Ma, Y. (1999). Comparative analysis of exclusionary rules in the United States, England, France, Germany, and Italy. *Policing: An International Journal of Police Strategies & Management, 22*, 280–203.

McQuade, S. (2006). Technology-enabled crime, policing and security. *Journal of Technology Studies, 32*, 32–42.

National Institute of Justice, United States Department of Justice. (2008). Electronic crime scene investigation: A guide for first responders. Washington, DC: U.S. Department of Justice.

Nzjboer, J. F. (2000). Methods of investigation and exclusion of evidence: A comparative and interdisciplinary perspective. In J. F. Nijboer & W. J. J. M. Sprangers (Eds.), *Harmonisation in forensic expertise* (pp. 431–446). Amsterdam: Thela Thesis.

Pattenden, R. (2009). Authenticating 'Things' in English law: Principles for adducing tangible evidence in common law jury trials. *The International Journal of Evidence & Proof, 12*, 273–302.

Pradel, J. (2000). Criminal evidence. In J. F. Nijboer & W. J. J. M. Sprangers (Eds.), *Harmonisation in forensic expertise: An inquiry into the desirability of and opportunities for international standards* (pp. 411–429). Amsterdam: Thela Thesis.

Pugh, G. W. (1962). Administration of criminal justice in France: An introductory analysis. *Louisiana Law Review, 23*, 1–28.

Reed, C. (1990). The admissibility and authentication of computer evidence-a confusion of issues. *Computer Law & Security Report, 6*, 13–16.

Rengel, A. (2013). *Privacy in the 21st century*. Leiden: Martinus Nijhoff.

Rentschler, C. A. (2016). Technologies of Bystanding: Learning to see like a Bystander. In S. Pearl (Ed.), *Images, ethics, technology* (pp. 15–40). New York: Rutledge.

Roberts, P., & Zuckerman, A. (2010). *Criminal evidence*. Oxford: Oxford University Press.

Shifrin, O. S. (1991). Fourth amendment--protection against unreasonable search and seizure: The inadequacies of using an anonymous tip to provide reasonable suspicion for an investigatory stop. *Journal of Criminal Law and Criminology, 81*, 760–778.

Solon, M., & Harper, P. (2004). Preparing evidence for court. *Digital Investigation, 1*, 279–283.

Sopinka, J. (1999). *The law of evidence in Canada*. Toronto: Butterworths.

Stannard, G. M. (2015). The Liar and the Loophole: Corporate character evidence and impeachment. *Brooklyn Law Review, 81*, 239–267.

Stephen, J. (1886). *A digest of the law of evidence*. London: William Clowes & Sons.

Thayer, J. (1898). *A preliminary treatise on evidence at the common law*. Boston: Little, Brown & Co..

The Law Commission. (1995). *Evidence in criminal proceedings: Hearsay and related topics*. London: HMSO.

Thomson, L. L. (2013). Mobile devices new challenges for admissibility of electronic evidence. *The SciTech Lawyer, 9*, 1–5.

Tillers, P., & Schum, D. (1991). A theory of preliminary fact investigation. *Davis Law Review, 24*, 931–1012.

Universal Declaration of Human Rights. (1948, December 10). United Nations General Assembly (UNGA) Res 217 A (III).

Wigmore, J. H. (1942). The American law institute code of evidence rules: A dissent. *American Bar Association Journal, 28*, 23–28.

Williams, K. (1998). Do we really need the federal rules of evidence? *North Dakota Law Review, 74*, 1–34.

Woods, D. C. (1931). The French Court of Assizes. *American Institute of Criminal Law and Criminology, 22*, 325–334.